Arkose Labs

8 Trends Fueling Account Takeover Attacks on Fintechs

How Fraud and Security Teams are Navigating an Increasingly Complex Threat Landscape

The New Face Of Financial Services

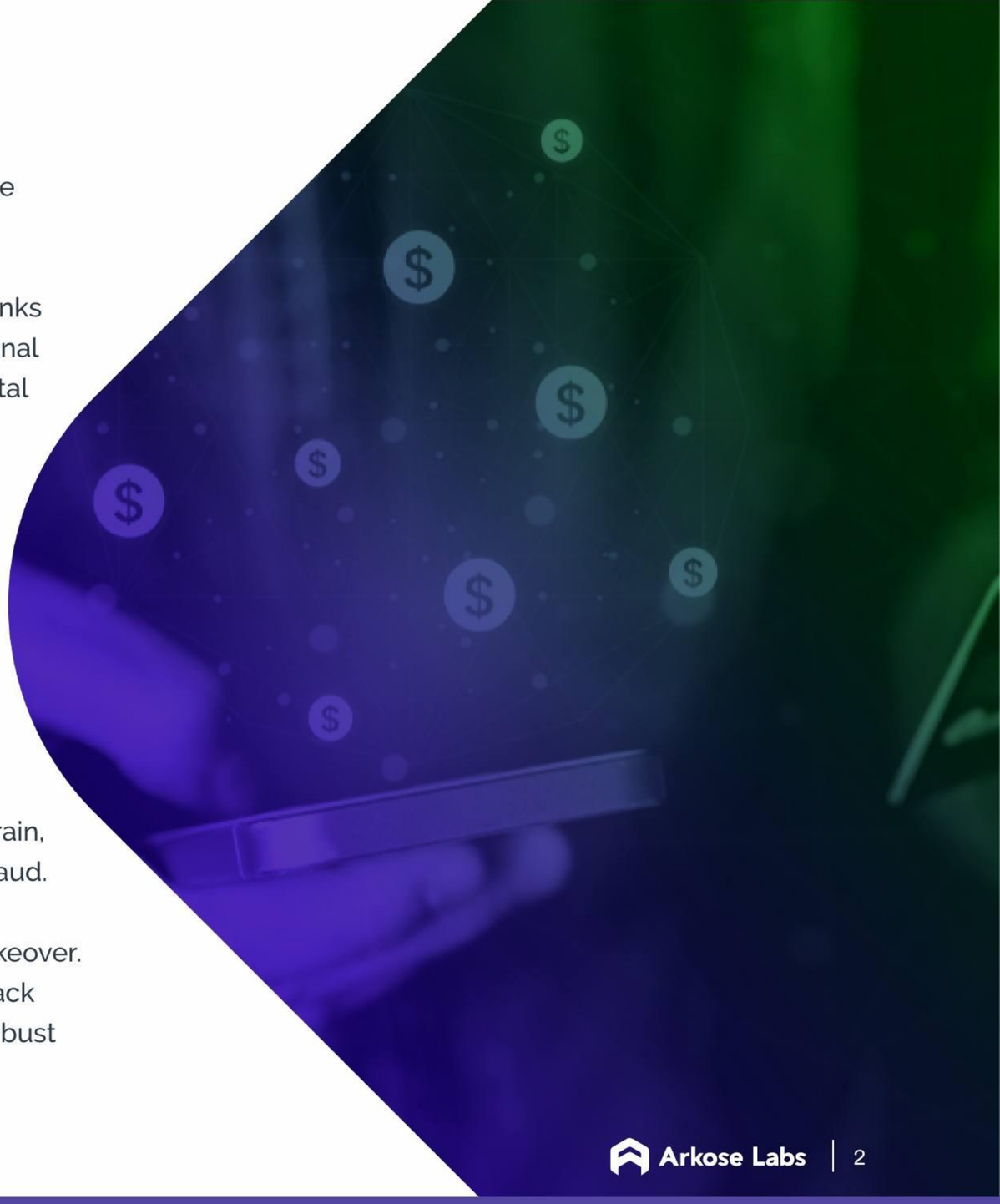
An industry like no other, fintech is an engine of innovation that is rewriting the rule book on how consumers around the globe access financial services.

A wide array of dynamic providers have emerged, with digital and mobile-only banks and online lenders making the biggest splash. Lines are blurring between traditional banking and fintech, with more and more brick-and-mortar banks embracing digital services and integrating with fintechs through open banking.

A major impact of the fintech revolution has been the speed at which banking and lending decisions are made, with consumers expecting instant access to new financial products. This presents unique challenges when protecting their digital properties against organized fraud.

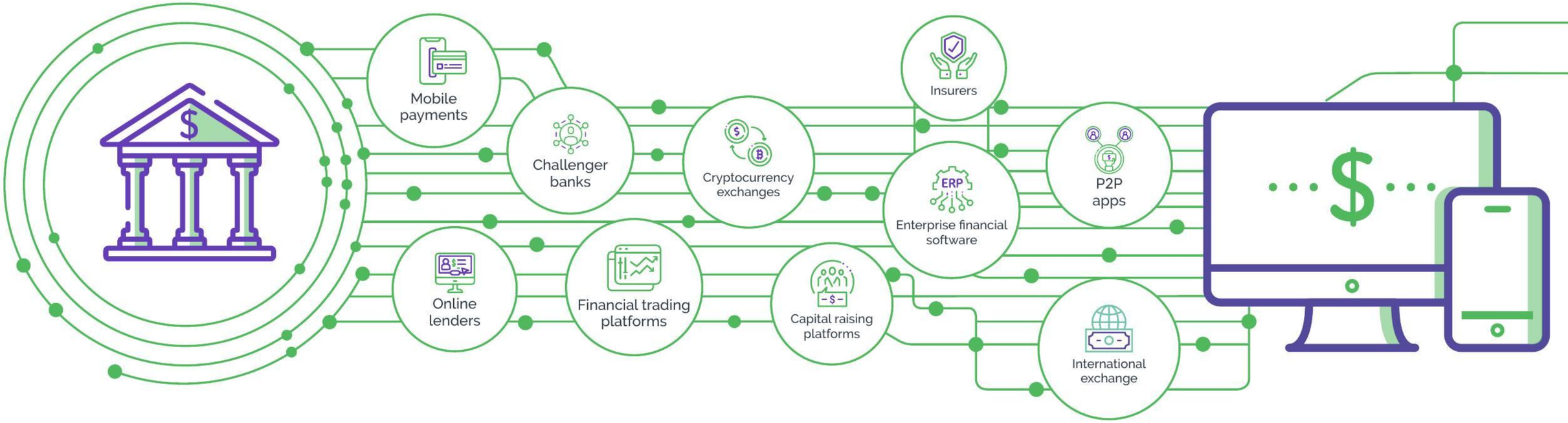
Fintechs face a complex and highly organized cybercrime ecosystem. The 2019 Official Annual Cybercrime Report predicted that by 2021 cybercrime will cause annual losses of $6 trillion globally. The high ROI potential for attackers targeting the finance sector means that internal fraud prevention teams are under major strain, both mentally and monetarily, as they keep up with the ever-evolving nature of fraud.

A top fraud and security issue which fintechs are dealing with today is account takeover. Legitimate consumers are having accounts compromised through an array of attack techniques, including large-scale automated credential stuffing. Fintechs need robust protection in place, which is in line with their commitment to user experience.



1 An Explosion In Banking And Lending Start-Up Capital

The evolving fintech landscape provides highly-coveted, innovative and user-focused alternatives to legacy banking options, offering cost savings and better ROI. They are both in competition and "coopetition" with traditional financial institutions and are highly sought-after in the private equity markets, with global venture capital investments of over $52B in H1 '21 driving the fintech surge. 2021 is shaping up to be a record-breaking year for fintech IPOs due to the pandemic, which has sparked unprecedented growth.

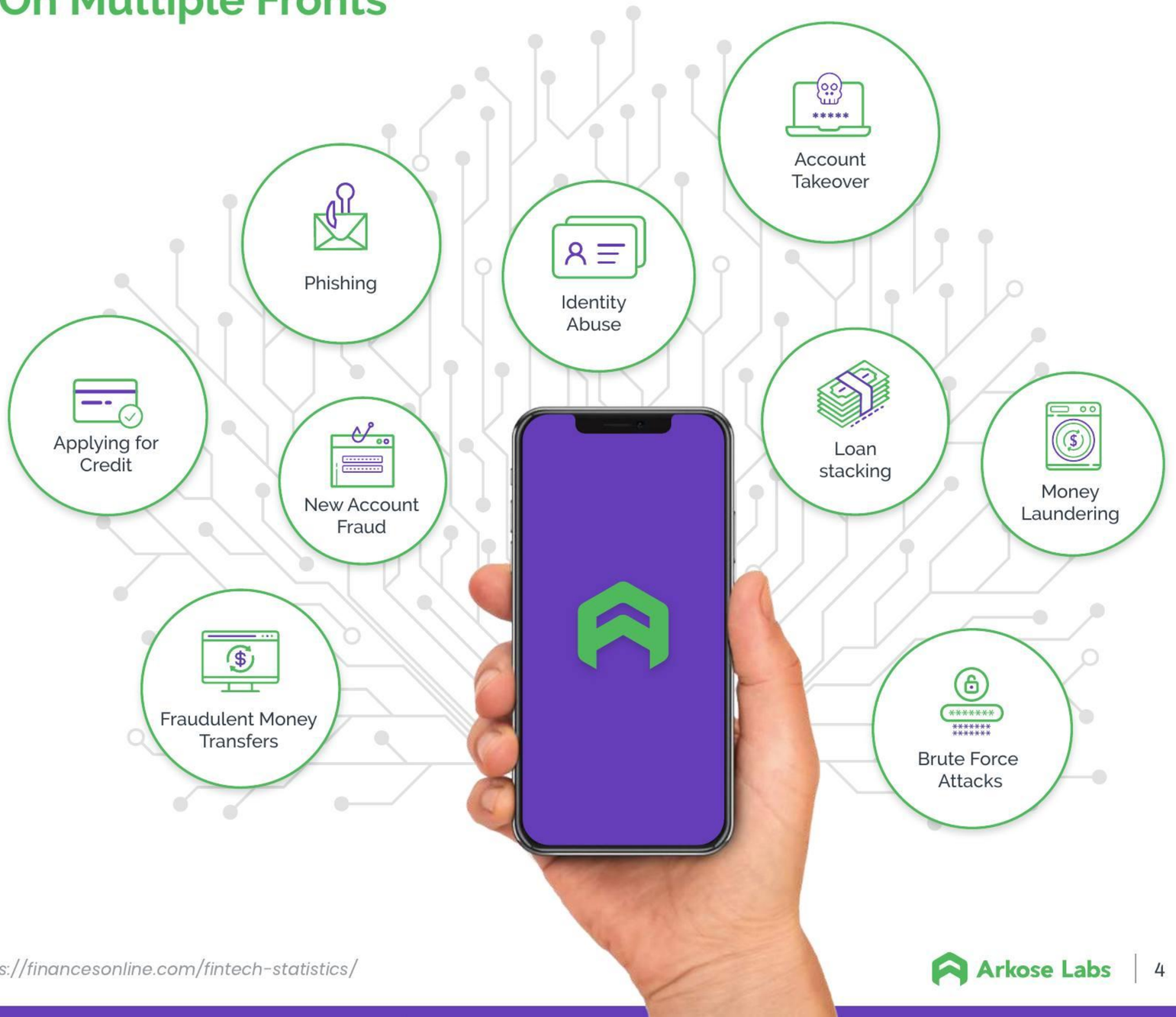


KPMG Pulse of Fintech H1'21: *https://home.kpmg/xx/en/home/insights/2021/08/pulse-of-fintech-h1-2021-global.html*

2 Fintechs Face Attacks On Multiple Fronts

The global fintech market is predicted to grow to $310 billion at an annual growth rate of 24.8% through 2022*. This offers a wealth of positive aspects for customers worldwide, but also increases the attack surface for attackers targeting financial transactions.

A shadow cybercrime ecosystem has expanded to attack these businesses from every angle. Attackers have developed sophisticated attack patterns that confound traditional fraud and account security solutions. They learn from previous failed attacks and invest considerable resources in staying ahead of security strategies.



*Research and Markets Global Fintech Market Report 2020 - https://financesonline.com/fintech-statistics/

3 The High Stakes Game Of Account Takeover

Accessing financial accounts through account takeover allows fraudsters to commit serious cybercrimes, affecting both individual users and wider society.

Money laundering and money muling Fund organized crime Password and payment details theft Fraudulent credit applications Account draining.

Attackers are using stolen data and corrupted digital identities to mount attacks at scale. Highly sophisticated bots easily bypass traditional fraud prevention solutions using data harvested from previous failed attempts to evolve and improve.

Additionally, as security technology evolves, criminals are increasingly employing cheap human labor in developing economies to turbo-charge attacks. Arkose Labs found that human-driven attacks increased six fold in the first half of 2020.

Businesses today need a multi-layered approach that differentiates between human and bot-driven account fraud to maximize cost savings and generate a better return on investment.

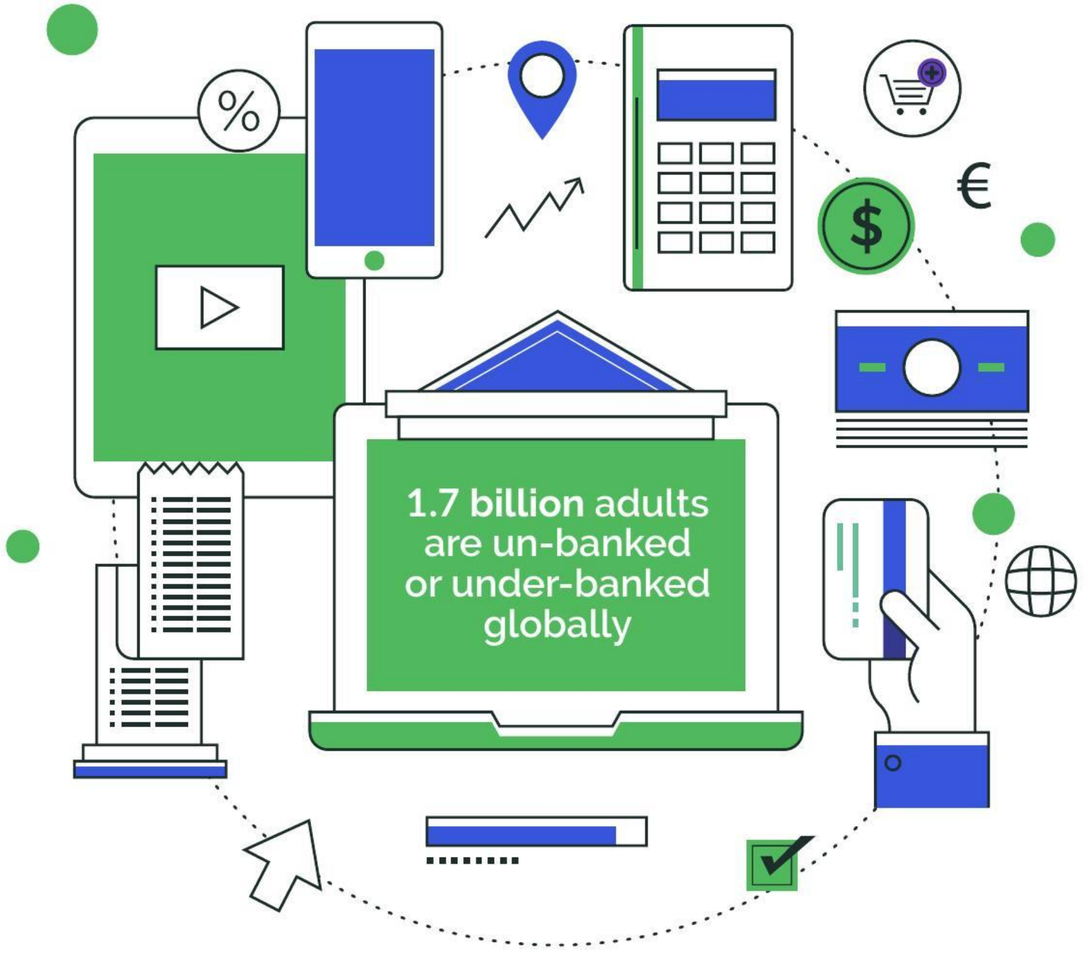
4 Fintechs Are Driving Global Financial Inclusion

Fintechs can offer financial services to individuals typically excluded from traditional banking.

The issue of un-banked and under-banked individuals is a major obstacle to social mobility and financial stability. Fintechs are uniquely positioned to be able to expand access to financial services to these individuals. With lower overheads than traditional banking, they can tap into this global market by offering low-cost products to individuals, including micro-loans, investment and financial risk management.

Where thin-file individuals have little or no credit history, fintechs can access data from vendors' real-time transactions on commercial platforms allowing them to assess risk on a micro-basis. Through e-payments and money transfer services, fintechs can offer quick, low- cost transfers that provide large savings for those with the biggest need. This has a huge impact on individuals working abroad and sending money home to less-economically stable countries.

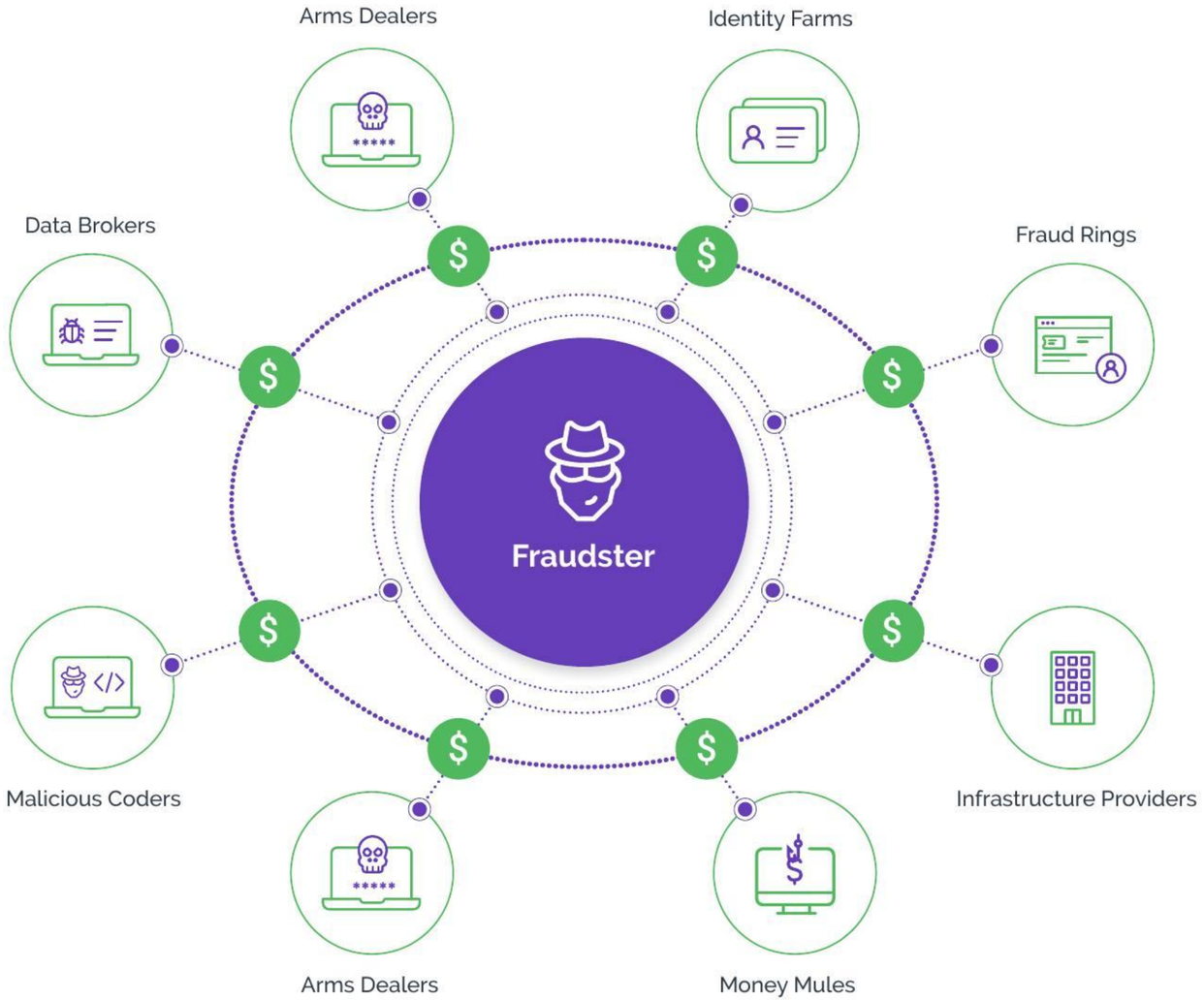
Global digital intelligence is playing a vital role in opening financial services up to the least privileged, and encouraging growth in developing economies.



5 Start-Ups Versus A Mature Global Cybercrime Ecosystem

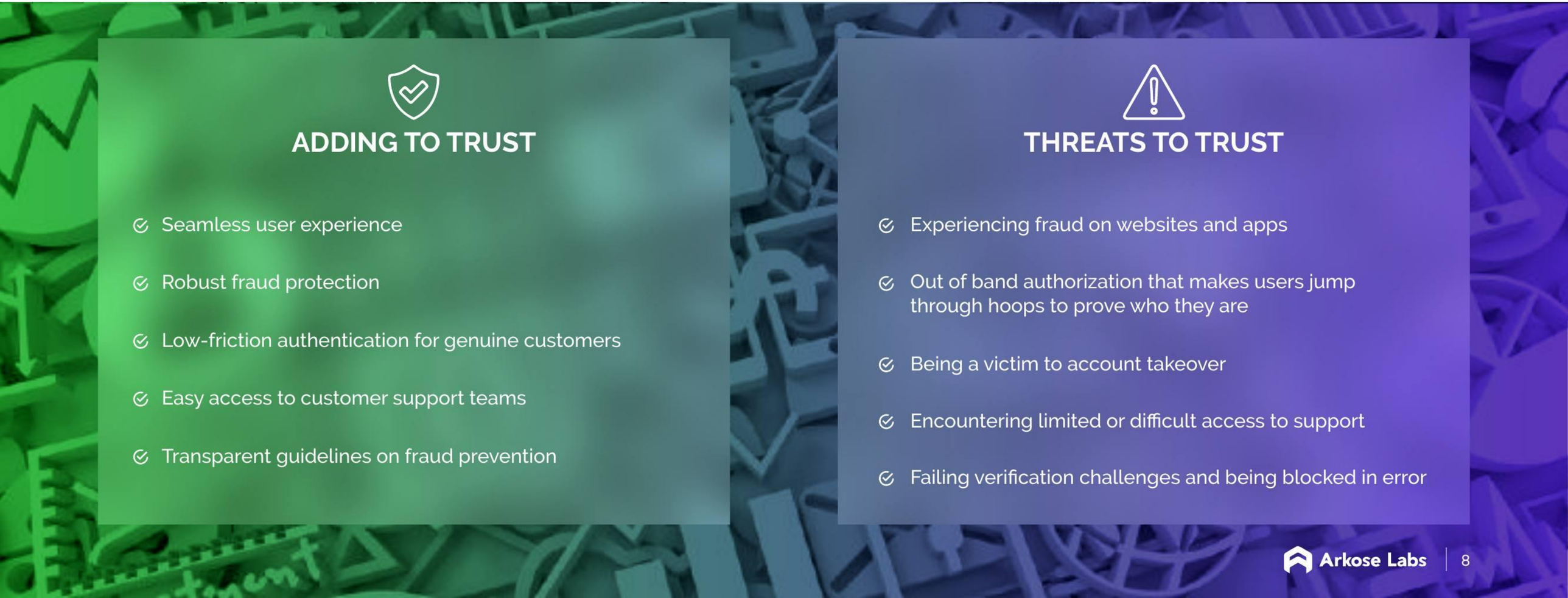
Fast-growth fintechs are facing a well developed, inter-connected cybercrime ecosystem, which has honed its tactics and techniques after years of targeting traditional financial institutions.

Attackers can tap into a range of services and data for sale: identity farms, which provide verified, complete identity profiles; vendors of sophisticated fraud toolkits; and sweatshops offering human resources to carry out attacks from low-cost regions such as South East Asia. Additionally, attackers have developed highly effective bots that mimic human activity and easily bypass traditional fraud and security solutions.



6 Building And Preserving Trust In Fintech

As challenger banks and online lenders strive to establish credibility, competing with established institutions who have dominated the market for decades, establishing and maintaining customer trust is 100% central to their commercial success. By providing cost-effective, secure services that yield better ROI, these challenger banks and online lenders can build trust and establish their legitimacy in the market. Every interaction consumers have with these new services goes to either build or erode trust, and ultimately, the success of the business.



ADDING TO TRUST

- Seamless user experience
- Robust fraud protection
- Low-friction authentication for genuine customers
- Easy access to customer support teams
- Transparent guidelines on fraud prevention

THREATS TO TRUST

- Experiencing fraud on websites and apps
- Out of band authorization that makes users jump through hoops to prove who they are
- Being a victim to account takeover
- Encountering limited or difficult access to support
- Failing verification challenges and being blocked in error

7 Digital Identities Have Been Corrupted At Scale

As exclusively online and mobile businesses, fintechs are more reliant than other sectors on verifying the identity of users, without onerous identity proofing processes.

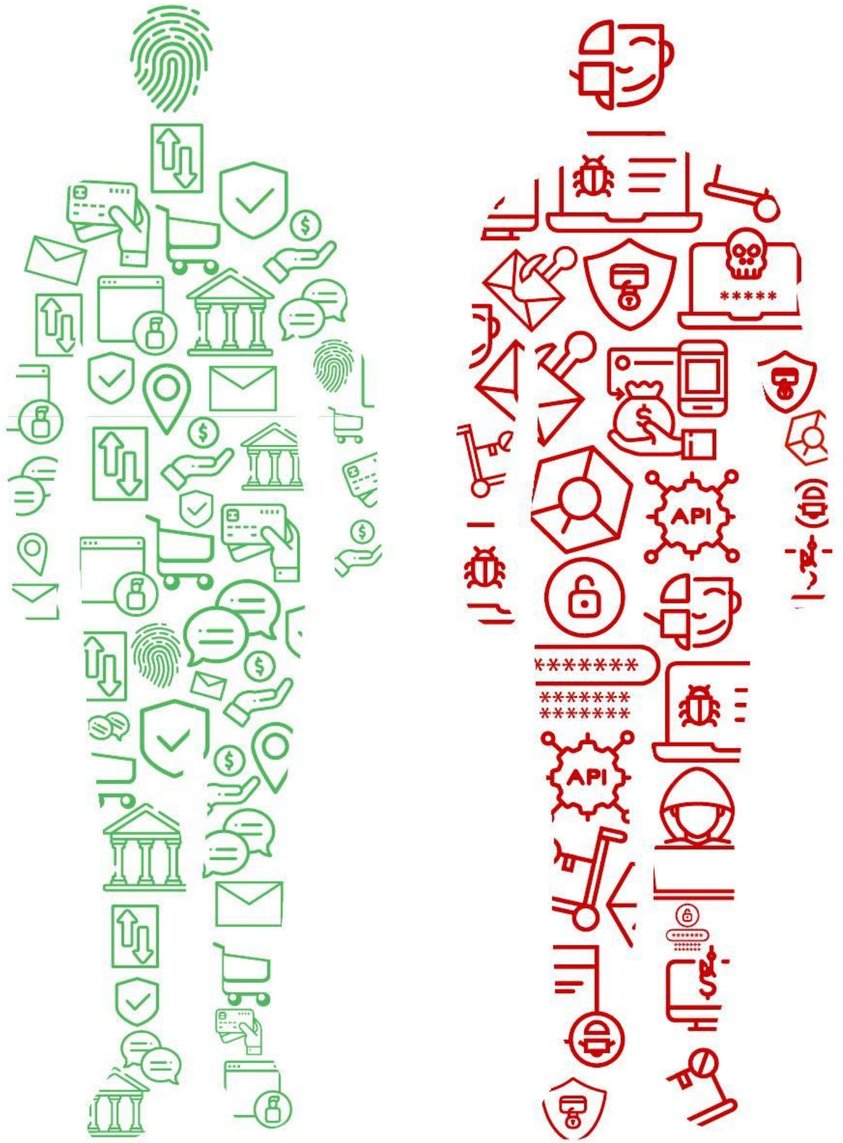
However, digital identity information has largely been compromised. Armed with accurate knowledge of the fraud detection parameters used to identify online abuse, attackers are able to use their own defenses against the businesses they attack in order to masquerade convincingly as trusted consumers.

Breached identity credentials: Fraudsters use wholesale 'identity farms' to access large pools of stolen and synthesized identity credentials.

Device intelligence: Fraudsters purchase cloned fingerprints of trusted devices to mimic good users, or use randomization tools to make stolen devices seem new.

IP address & location: Fraudsters use increasingly sophisticated location spoofing tools that enable them to appear as if they are a trusted source.

Behavior analytics: Fraudsters gain insight into the behavior patterns of genuine customers from previous account takeover and use attempts, and use this to circumvent anti-fraud measures.

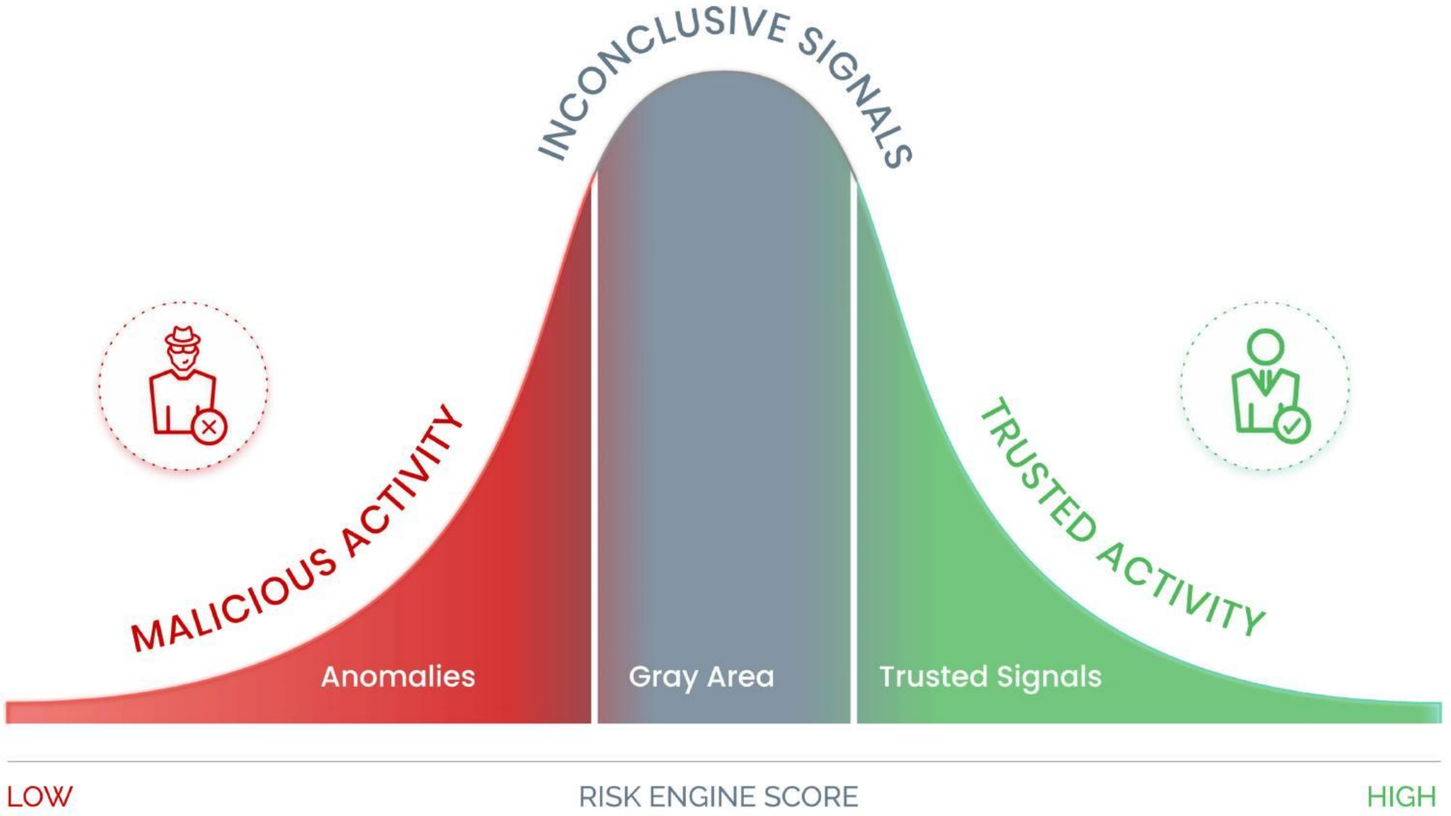


8 Navigating Unpredictable Fraud Signals In A Complex Threat Landscape

The corruption of digital identities makes it difficult to accurately differentiate between consumers and attackers purely through data-driven analysis. There is a growing 'gray area' between traffic that is recognized as trusted and that which is fraudulent.

Attackers have data at their disposal and highly developed tools that can deceive traditional fraud and security solutions. Genuine consumers can also display unpredictable behavior.

Fintechs are set up to process high numbers of applications quickly, and approve transactions in an automated, hands-off way, resulting in significant cost savings. The growing gray area means that it is increasingly difficult to achieve this without leaving the business vulnerable to fraud or placing a heavy burden on in-house teams.



Protecting Fintech Accounts From ATO

Fintech has opened up many avenues in the world of finance and as a result has become a lucrative target for fraudsters, who will always chase the money. Spurred on by the rapid expansion of the sector, fraudsters are developing increasingly sophisticated attack patterns.

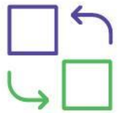
Fast-growth organizations are struggling to keep on top of the fight against fraud and account takeover attacks in a way that is sustainable and avoids a never-ending cat and mouse game with attackers. In order to disrupt account takeover in the long-term, fintechs need to address the economic drivers behind attacks. If a fraudster meets enough resistance, though controls which cannot be circumvented at scale through automation, they will abandon attacks before their ROI is completely eroded.

Businesses need to combine sophisticated risk decisioning, which digs deep for even the most subtle signs of fraud, with intelligent step-up authentication that adapts to the risk profile of traffic. To avoid getting bogged down by complexity, fraud and security solutions need to be integrated into existing frameworks and build trust with genuine users - without introducing unnecessary friction.

Fintechs can stay ahead of emerging attack patterns and stamp out large-scale attacks from bots and malicious humans by deploying constantly evolving authentication steps. This not only provides better protection, but also helps them to achieve cost savings and improved ROI.

The Arkose Advantage

Arkose Labs has been designed to combat fraud and account takeover in the post-breach era. Its AI-powered platform combines real-time risk assessment with dynamic attack response to defeat persistent bots and co-ordinated human attacks on the most targeted user action points on fintech platforms. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response that deters future attempts and creates a more secure experience for genuine customers. Arkose Labs' multi-step defenses work together seamlessly to significantly increase labor involved in clearing challenges, resulting in cost savings and improved ROI for fintech platforms. This breaks the business model behind organized fraud, and creates a continuous feedback loop to ensure these platforms stay ahead of evolving threats long term.



Intermediary Platform Buffers Attacks
Independent verification of the authenticity of traffic to shift the attack surface.

Protects Against Automated Attacks
Robust anti-automation provides a commercial guarantee against all automated attacks.

Lightening-Fast Deployment
Cuts through the complexity with a solution that is easy to install and simple to manage.

Drains Fraudsters' Time and Resources
Renders attacks more difficult and costly to fraudsters, which disrupts their economic incentives.

Continuous Intelligence
Helps the fraud and risk management ecosystem by learning from new attack patterns and providing insights into fraud operations.

Zero-Tolerance Approach
Prevents fraudsters from bypassing its platform at scale using automation or fraud farms.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with a dynamic attack response that undermines the ROI behind attacks while improving good-user throughput and saving businesses money. Headquartered in San Mateo CA, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast 500 ranking.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Schedule Demo